

日本国特許庁
JAPAN PATENT OFFICE

別紙添付の書類に記載されている事項は下記の出願書類に記載されている事項と同一であることを証明する。

This is to certify that the annexed is a true copy of the following application as filed with this Office

出願年月日

Date of Application:

2002年12月19日

出願番号

Application Number:

特願2002-367460

[ST.10/C]:

[JP2002-367460]

出願人

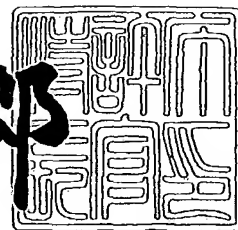
Applicant(s):

株式会社メルコ

2003年 1月21日

特許庁長官
Commissioner,
Japan Patent Office

太田信一郎



出証番号 出証特2002-3107630

【書類名】 特許願

【整理番号】 PA10F494

【提出日】 平成14年12月19日

【あて先】 特許庁長官 太田 信一郎 殿

【国際特許分類】 H04L 12/00

【発明者】

【住所又は居所】 名古屋市南区柴田本通4丁目15番 株式会社メルコ
ハイテクセンター内

【氏名】 石徹白 敬

【特許出願人】

【識別番号】 390040187

【氏名又は名称】 株式会社メルコ

【代理人】

【識別番号】 110000028

【氏名又は名称】 特許業務法人 明成国際特許事務所

【代表者】 下出 隆史

【電話番号】 052-218-5061

【手数料の表示】

【予納台帳番号】 133917

【納付金額】 21,000円

【提出物件の目録】

【物件名】 明細書 1

【物件名】 図面 1

【物件名】 要約書 1

【包括委任状番号】 0108819

【プルーフの要否】 要

【書類名】 明細書

【発明の名称】 暗号鍵設定システム、アクセスポイント、および、暗号鍵設定方法、認証コード設定システム

【特許請求の範囲】

【請求項1】 無線LAN用の中継器であるアクセスポイントと無線LAN接続用デバイスを備えた端末との間で無線で通信される無線通信データを通信に先立って暗号化する際に用いられる暗号鍵を、前記端末に設定する暗号鍵設定システムであって、

前記アクセスポイントと前記端末との間の無線通信範囲を通常の通信範囲よりも狭める通信範囲限定手段と、

該通信範囲限定手段により無線通信範囲が狭められたとき、該通信範囲内に存在する端末と該アクセスポイントとの間で、前記暗号鍵の内容を表わす暗号鍵データを無線で通信することにより前記暗号鍵を設定する暗号鍵設定手段とを備えた暗号鍵設定システム。

【請求項2】 請求項1に記載の暗号鍵設定システムであって、前記アクセスポイントに対して前記暗号鍵の設定開始を指示する指示手段と、該指示手段により指示に基づいて前記無線通信範囲を通常の通信範囲よりも狭める条件を決定する条件決定手段とを備え、

前記通信範囲限定手段は、該条件決定手段により決定された条件下で、前記無線通信範囲を狭める手段である暗号鍵設定システム。

【請求項3】 請求項1または2に記載の暗号鍵設定システムであって、前記通信範囲限定手段は、前記アクセスポイントが、前記端末から暗号鍵を設定する旨の指示を受信する際に、無線通信範囲を通常の通信範囲よりも狭める制御を行ない、

前記無線設定手段による暗号鍵の設定が終了したときに、無線通信範囲を通常の通信範囲に戻す制御を行なうことによって実現される暗号鍵設定システム。

【請求項 4】 前記通信範囲限定手段は、前記アクセスポイントの送信出力を調整することにより前記無線通信範囲を狭める手段である請求項 1 ないし 3 のいずれかに記載の暗号鍵設定システム。

【請求項 5】 前記通信範囲限定手段は、前記暗号鍵の設定が行なわれる端末およびアクセスポイントを前記無線信号に対して遮蔽する遮蔽体である請求項 1 に記載の暗号鍵設定システム。

【請求項 6】 前記アクセスポイントは、通信対象となる端末に固有の情報を登録する登録手段を備えた請求項 1 ないし 5 のいずれかに記載の暗号鍵設定システム。

【請求項 7】 無線 LAN 接続用デバイスを備えた端末との間で無線での通信を行なう無線 LAN 用の中継器であって、前記端末との無線での通信に先立って、設定された暗号鍵を用いて通信対象となる無線通信データを暗号化し、該暗号化された無線通信データを用いて前記端末との無線通信を行なうアクセスポイントであって、

前記端末との間の無線通信範囲を通常の通信範囲よりも狭める通信範囲限定手段と、

該通信範囲限定手段により無線通信範囲が狭められたとき、該通信範囲内に存在する端末との間で、前記暗号鍵の内容を表わす暗号鍵データを無線で通信することにより前記暗号鍵を設定する暗号鍵設定手段と

を備えたアクセスポイント。

【請求項 8】 無線 LAN 用の中継器であるアクセスポイントと無線 LAN 接続用デバイスを備えた端末との間で無線で通信される無線通信データを通信に先立って暗号化する際に用いられる暗号鍵を、前記端末に設定する方法であって、

前記アクセスポイントと前記端末との間の無線通信範囲を通常の通信範囲よりも狭め、

該無線通信範囲が狭められたとき、該通信範囲内に存在する端末と該アクセスポイントとの間で、前記暗号鍵の内容を表わす暗号鍵データを無線で通信することにより前記暗号鍵を設定する。

暗号鍵設定方法。

【請求項 9】 無線 LAN 接続用デバイスを備えた端末が無線 LAN 用の中継器であるアクセスポイントに無線で通信してネットワーク上の所定のデータにアクセスする際に要求される認証コードを、前記端末および前記アクセスポイントのうちの少なくとも一方に設定する認証コード設定システムであって、

前記アクセスポイントと前記端末との間の無線通信範囲を通常の通信範囲よりも狭める範囲限定手段と、

該通信範囲限定手段により無線通信範囲が狭められたとき、該通信範囲内に存在する端末と該アクセスポイントとの間で、前記認証コードの内容を表わすデータを無線で通信することにより前記認証コードを設定する設定手段と

を備えた認証コード設定システム。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】

本発明は、無線 LAN 用の中継器であるアクセスポイントと無線 LAN 接続用デバイスを備えた端末との間で無線で通信される無線通信データを通信に先立って暗号化する際に用いられる暗号鍵を、前記端末および前記アクセスポイントに設定する技術に関する。

【0002】

【従来の技術】

近年、無線 LAN 用の中継器であるアクセスポイントは、離れた位置にある複数のコンピュータをインターネットに接続するデバイスとして、自宅やオフィス内等の特定人が継続的に活動する場所（以下、プライベートスペースという）のみならず、ホテルや空港、商店街、公園、駅等の不特定多数の人が一時的に活動する場所（以下、パブリックスペースという）でも利用され始めている。例えば、アクセスポイントを、xDSL 回線や CATV 回線等の高速なインターネット接続サービスを実現するブロードバンド回線に接続してパブリックスペースに配置することにより、アクセスポイントから発信された電波が届く範囲（無線通信エリア）内にいる不特定多数人に対して自由にインターネットに接続できる空間

(以下、フリースポットという)を提供するサービスが提案されている。即ち、パブリックスペースの管理者が加入しているブロードバンド回線を、無線LAN用のアクセスポイントを用いてパブリックスペースの利用者が所持する端末に開放するのである。これにより、利用者によるインターネット接続の利便性が高まり、パブリックスペースの利用促進を図ることができる。

【0003】

このようなフリースポットでは、無線通信エリア内での無線LANを介したインターネットへの接続権限を、限定者(例えば、お得意様)のみに認める場合があり、こうした場合には、限定者以外の人によるネットワークへの不正侵入を防止する必要があった。また、多数の人が集まるフリースポットでは、各人が所持する端末とアクセスポイントとの間で無線通信用の電波が頻繁に飛び交うので、多数の各人のプライバシーを十全に保護するために、無線通信エリア内での電波の傍受により通信内容が第三者に漏洩することを確実に防止する必要があった。

【0004】

一方、無線LANに関しては、従来、ネットワークへの不正侵入や通信内容の第三者への漏洩を防止するセキュリティ技術が種々提案されていた。例えば、端末に装着される無線LAN接続用デバイス(例えば、無線LANアダプタ)に予め割り当てられた固有の識別番号であるMAC(Media Access Control)アドレスを利用し、このMACアドレスをアクセスポイントに登録しておき、端末からのアクセスに伴ってアクセスポイントがMACアドレスの認証を行ない、登録されたMACアドレス以外のMACアドレスであれば、該端末からのネットワークへの接続要求を拒否する技術(以下、MACアドレス制限という)が提案されていた(例えば、特許文献1を参照)。また、端末およびアクセスポイントに、共通の暗号鍵としてWEP(Wired Equivalent Privacy)キーを設定しておき、端末とアクセスポイントとの間でやりとりされるデータの内容をWEPキーを用いて暗号化し、データが漏洩した場合であっても、データの内容を解析しにくくし、データの内容がわからないようにする技術(以下、WEP暗号化という)も提案されていた(例えば、特許文献2を参照)。

【0005】

【特許文献1】

特開2001-320373号公報

【特許文献2】

特開2001-345819公報

【0006】

よって、セキュリティが確保されたフリースポットを実現するためには、フリースポットの利用に先立って、フリースポットを利用しようとする各人の端末について、MACアドレスの登録やWEPキーの設定を行なっておく必要があった。

【0007】

【発明が解決しようとする課題】

しかしながら、上記した従来のセキュリティ技術では、アクセスポイントへのMACアドレスの登録や端末へのWEPキーの設定を手作業で行なわなければならない、無線LANを利用する端末を新たに追加しようとする場合に煩雑かつ不便であるという課題があった。特に、パブリックスペースに設けられるフリースポットでは、フリースポットを利用しようとする者が多数存在し、しかも徐々に増えていく。このような多数の各端末所有者に、フリースポットを利用する条件として、MACアドレスの登録やのWEPキーの設定に関する端末操作を課すことは、極めて不便であり、現実的でなかった。

【0008】

また、端末側で任意の文字列を用いて設定されたWEPキーをアクセスポイント側にも設定するためには、無線LANを利用して設定すること、即ち、端末からWEPキーのデータを電波に乗せてアクセスポイントに無線で送信し、これを受信したアクセスポイントが当該端末についてのWEPキーを設定することが合理的である。こうすれば、端末所有者は、WEPキーの送信後すぐに、無線LANを介した各種のサービス（例えば、インターネット接続）を利用することができるからである。このようにWEPキーを無線で送信した場合には、端末とアクセスポイントとの間での電波の傍受によりWEPキーが第三者に漏洩するおそれ

がある。この場合、漏洩したWEPキーを手にした第三者は、WEPキーが設定された端末とアクセスポイントとの間でやり取りされる全てのデータを解析してデータの内容を知ることが可能となり、これでは暗号化によるセキュリティシステムが機能しなくなってしまう。特に、フリースポットのアクセスポイントでは、フリースポットを利用しようとする多数の者の端末についてWEPキーの設定が行なわれるので、WEPキーの漏洩を十全に防止し、多数の各利用者の通信の秘密を十全に確保する必要がある。

【0009】

そこで、本発明は、上記の課題を解決し、無線LANを利用する端末の新規追加を、暗号鍵を表わすデータの漏洩を防止しつつ、簡便な手法で実現することを目的として、以下の構成を採った。

【0010】

【課題を解決するための手段およびその作用・効果】

本発明の暗号鍵設定システムは、

無線LAN用の中継器であるアクセスポイントと無線LAN接続用デバイスを備えた端末との間で無線で通信される無線通信データを通信に先立って暗号化する際に用いられる暗号鍵を、前記端末に設定する暗号鍵設定システムであって、

前記アクセスポイントと前記端末との間の無線通信範囲を通常の通信範囲よりも狭める通信範囲限定手段と、

該通信範囲限定手段により無線通信範囲が狭められたとき、該通信範囲内に存在する端末と該アクセスポイントとの間で、前記暗号鍵の内容を表わす暗号鍵データを無線で通信することにより前記暗号鍵を設定する暗号鍵設定手段と

を備えたことを要旨とする。

【0011】

上記の無線LAN接続用デバイスは、端末とアクセスポイントとの間での無線通信を行なえるようにするために、端末に装着されるデバイスである。この無線LAN接続用デバイスの一例として、無線LANアダプタや無線LANカードを考慮することができる。

【0012】

本発明の暗号鍵設定システムでは、アクセスポイントと端末との間で通信される無線通信データを暗号化する際に用いられる暗号鍵を設定する。こうした暗号鍵の設定は、アクセスポイントと端末との間の無線通信範囲が通常の通信範囲よりも狭められたとき、該端末と該アクセスポイントとの間で、暗号鍵の内容を表わす暗号鍵データを無線で通信することにより行なわれる。こうすれば、暗号鍵データを無線で通信した場合であっても、暗号鍵データはアクセスポイントを中心とした狭い範囲でやり取りされるので、暗号鍵データが乗った無線の傍受がしにくくなり、暗号鍵データの漏洩が防止される。従って、無線LANを利用する端末の新規追加を、暗号鍵データの漏洩を防止しつつ、簡便に実現することが可能となり、加入し易い無線LANを高いセキュリティレベルで実現することができる。

【 0 0 1 3 】

通信範囲限定手段を実現する態様として、種々の態様を考えることができる。例えば、アクセスポイント側で実現することも可能である。具体的には、アクセスポイントに対して前記暗号鍵の設定開始を指示する指示手段と、該指示手段により指示に基づいて前記無線通信範囲を通常の通信範囲よりも狭める条件を決定する条件決定手段とを備え、前記通信範囲限定手段を、該条件決定手段により決定された条件下で、前記無線通信範囲を狭める手段としてもよい。こうすれば、暗号鍵の設定開始が指示された場合に、この指示に基づいて決定された条件下で無線通信範囲が狭められ、暗号鍵の設定がなされる。従って、アクセスポイントを、常時、暗号鍵の設定を受け付ける状態にしておく必要がない。

【 0 0 1 4 】

アクセスポイントが、端末から暗号鍵を設定する旨の指示を受信する際に、無線通信範囲を通常の通信範囲よりも狭める制御を行ない、無線設定手段による暗号鍵の設定が終了したときに、無線通信範囲を通常の通信範囲に戻す制御を行なうこととしてもよい。こうすれば、端末の所有者は、暗号鍵の設定をアクセスポイントに触れることなく行なうことが可能となる。また、通信範囲限定手段を、アクセスポイントの送信出力を調整することにより前記無線通信範囲を狭める手段としてもよい。

【 0 0 1 5 】

通信範囲限定手段を、前記暗号鍵の設定が行なわれる端末およびアクセスポイントの前記無線信号に対して遮蔽する遮蔽体とすることも可能である。こうすれば、暗号鍵データが乗った無線（以下、暗号鍵無線という）が遮蔽体の外部に送出されたり、暗号鍵無線を傍受するための無線が遮蔽体の内部に侵入したりすることが確実に防止される。従って、暗号鍵データの第三者への漏洩を十全に防止することができる。

【 0 0 1 6 】

アクセスポイントが、通信対象となる端末に固有の情報を登録する登録手段を備えることとしてもよい。こうすれば、固有の情報が登録された端末についてのみ、無線LANへの接続を許容することが可能となり、接続権限のない者による無線LANへの接続を防止することができる。また、接続権限のない者がLAN上の端末やアクセスポイントに侵入して暗号鍵データ等の各種のデータを取得することを未然に防止することができる。

【 0 0 1 7 】

本発明のアクセスポイントは、

無線LAN接続用デバイスを備えた端末との間で無線での通信を行なう無線LAN用の中継器であって、前記端末との無線での通信に先立って、設定された暗号鍵を用いて通信対象となる無線通信データを暗号化し、該暗号化された無線通信データを用いて前記端末との無線通信を行なうアクセスポイントであって、

前記端末との間の無線通信範囲を通常の通信範囲よりも狭める通信範囲限定手段と、

該通信範囲限定手段により無線通信範囲が狭められたとき、該通信範囲内に存在する端末との間で、前記暗号鍵の内容を表わす暗号鍵データを無線で通信することにより前記暗号鍵を設定する暗号鍵設定手段と

を備えたことを要旨とする。

【 0 0 1 8 】

本発明のアクセスポイントでは、端末との間での通信対象となる無線通信データを暗号化する際に用いられる暗号鍵を無線で端末に通信し、端末に暗号鍵を設

定する。こうした暗号鍵の設定は、端末との間の無線通信範囲が通常の通信範囲よりも狭められたとき、該端末との間で、暗号鍵の内容を表わす暗号鍵データを無線で通信することにより行なわれる。こうすれば、暗号鍵データを無線で通信した場合であっても、暗号鍵データはアクセスポイントを中心とした狭い範囲でやり取りされるので、暗号鍵データが乗った無線の傍受がしにくくなり、暗号鍵データの漏洩が防止される。従って、無線LANを利用する端末の新規追加を、暗号鍵データの漏洩を防止しつつ、簡便に実現することが可能となり、加入しやすい無線LANを高いセキュリティレベルで実現することができる。

【 0 0 1 9 】

本発明の暗号鍵設定方法は、

無線LAN用の中継器であるアクセスポイントと無線LAN接続用デバイスを備えた端末との間で無線で通信される無線通信データを通信に先立って暗号化する際に用いられる暗号鍵を、前記端末に設定する方法であって、

前記アクセスポイントと前記端末との間の無線通信範囲を通常の通信範囲よりも狭め、

該無線通信範囲が狭められたとき、該通信範囲内に存在する端末と該アクセスポイントとの間で、前記暗号鍵の内容を表わす暗号鍵データを無線で通信することにより前記暗号鍵を設定することを要旨とする。

【 0 0 2 0 】

本発明の暗号鍵設定方法では、アクセスポイントと端末との間で通信される無線通信データを暗号化する際に用いられる暗号鍵を端末に設定する。こうした暗号鍵の設定は、アクセスポイントと端末との間の無線通信範囲が通常の通信範囲よりも狭められたとき、該端末と該アクセスポイントとの間で、暗号鍵の内容を表わす暗号鍵データを無線で通信することにより行なわれる。こうすれば、暗号鍵データを無線で通信した場合であっても、暗号鍵データはアクセスポイントを中心とした狭い範囲でやり取りされるので、暗号鍵データが乗った無線の傍受がしにくくなり、暗号鍵データの漏洩が防止される。従って、無線LANを利用する端末の新規追加を、暗号鍵データの漏洩を防止しつつ、簡便に実現することが可能となり、加入しやすい無線LANを高いセキュリティレベルで実現することが

できる。

【 0 0 2 1 】

本発明の認証コード設定システムは、

無線 LAN 接続用デバイスを備えた端末が無線 LAN 用の中継器であるアクセスポイントに無線で通信してネットワーク上の所定のデータにアクセスする際に要求される認証コードを、前記端末および前記アクセスポイントのうちの少なくとも一方に設定する認証コード設定システムであって、

前記アクセスポイントと前記端末との間の無線通信範囲を通常の通信範囲よりも狭める範囲限定手段と、

該通信範囲限定手段により無線通信範囲が狭められたとき、該通信範囲内に存在する端末と該アクセスポイントとの間で、前記認証コードの内容を表わすデータを無線で通信することにより前記認証コードを設定する設定手段と

を備えたことを要旨とする。

【 0 0 2 2 】

上記の認証コードとしては、アクセスポイントから有料情報を取得するために必要な個人情報（例えば、端末所有者の氏名、ID やパスワード等）等を考えることができる。

【 0 0 2 3 】

本発明の認証コード設定システムでは、端末がアクセスポイントに無線で通信してネットワーク上の所定のデータにアクセスする際に要求される認証コードを、端末およびアクセスポイントのうちの少なくとも一方に設定する。こうした認証コードの設定は、アクセスポイントと端末との間の無線通信範囲が通常の通信範囲よりも狭められたとき、該端末と該アクセスポイントとの間で、認証コードの内容を表わすデータ（以下、認証コードデータという）を無線で通信することにより行なわれる。こうすれば、認証コードデータを無線で通信した場合であっても、認証コードデータはアクセスポイントを中心とした狭い範囲でやり取りされるので、認証コードデータが乗った無線の傍受がしにくくなり、認証コードデータの漏洩が防止される。従って、無線 LAN を利用する端末に関する認証コードの設定を、認証コードデータの漏洩を防止しつつ、簡便に実現することが可能

となり、無線LANのセキュリティレベルを高めることができる。

【0024】

【発明の実施の形態】

以上説明した本発明の構成および作用を一層明らかにするために、以下本発明の実施の形態を、以下の順序で説明する。

A. 第1実施例（暗号鍵設定システムLH1）

A-1. 暗号鍵設定システムLH1の概要

A-2. WEPキーの設定に関する処理の内容

A-3. 作用効果

B. 第2実施例（暗号鍵設定システムLH2）

C. 変形例

【0025】

A. 実施例：

A-1. 暗号鍵設定システムLH1の概要：

図1は本発明の第1実施例である暗号鍵設定システムLH1を実現するハードウェアの構成を示す説明図であり、図2はアクセスポイント20の構成を示す説明図である。暗号鍵設定システムLH1は、無線LANの無線通信エリアAR1内において、端末50とアクセスポイント20との間で、暗号鍵としてのWEPキーの内容を表わすキーデータを電波に乗せて無線通信することにより、端末50にアクセスポイント20が使用するWEPキーを設定するシステムである。

【0026】

図1に示すように、無線通信エリアAR1には、無線LAN用の中継器であるアクセスポイント（無線基地局）20が設置されている。アクセスポイント20は、図2に示すように、CPU11と、このCPU11とバスにより相互に接続されたROM12、RAM13、ハードディスク等の不揮発的な記憶装置14、ネットワークインタフェースとしてのWANポート17、有線LANとの接続用のLANポート22、無線通信インタフェース18、ディスプレイコントローラ15、入出力コントローラ16等の各部を備える。

【0027】

ROM12には、無線通信エリアAR1内の端末50、60、70との通信やインターネットINへの接続に関する各種のプログラムとこのプログラムの実行に必要なデータが格納されている。入出力コントローラ16にはプッシュ式の登録ボタン127が接続されている。登録ボタン127は、その押圧部がアクセスポイント20の筐体表面に露出した状態で設けられている。ディスプレイコントローラ15には、無線LANの接続状態や通信状態を点灯・点滅等によって表示する各種の表示ランプ19が接続されている。

【0028】

無線通信インタフェース18には、電波を送信する送信機25、電波を受信する受信機26が接続されている。この送信機25、受信機26は、外部への電波の送信や外部からの電波の受信が可能な状態で、アクセスポイント20に内蔵されている。図1では、送信機25の出力や受信機26の受信感度を標準設定値とした場合に、送信機25から送信された電波が届き、かつ、受信機26が端末50、60、70からの電波を受け取れる範囲を、無線通信エリアAR1として表わしている。こうしたアクセスポイント20の設置により、無線通信エリアAR1内を通常の通信範囲とした無線LANが組まれる。

【0029】

なお、ROM12には、端末50、60、70との通信に関するプログラムとして、送信機25の出力の標準設定値を一時的に変更する処理の内容が記述された出力値変更プログラムや受信機26の受信感度の標準設定値を一時的に変更する処理の内容が記述された受信感度値変更プログラムが予め格納されている。この設定値を変更する処理は、具体的には、標準設定値を $1/n$ （ n は予め定められた定数）倍する演算処理によって実現される。CPU11は、この出力値変更プログラム、受信感度値変更プログラムを実行することにより、変更後の出力値や受信感度値を、無線通信インタフェース18を介して送信機25、受信機26に出力する。これにより、送信機25から送信される電波の出力や受信機26における電波の受信感度に変更される。

【0030】

端末50、60、70は、周知のノート型のパーソナルコンピュータであり、

CPU、ROM、RAM等からなる制御装置をはじめ、記憶装置としてのハードディスクやCD-ROMドライブ等を備える。勿論、携帯情報端末（Personal Digital Assistant）等の他の端末であっても差し支えない。

【0031】

また、端末50、60、70には、アクセスポイント20との間での電波の送受信を行なえるようにする無線LAN接続用デバイスとして、無線LANアダプタ52、62、72が装着されている。この無線LANアダプタ52、62、72のデバイスドライバが端末50に組み込まれることにより、端末50、60、70は、装着された無線LANアダプタ52、62、72を認識し、無線LANアダプタ52、62、72を制御することが可能となる。なお、無線LANアダプタ52、62、72には、アダプタに固有の識別番号であるMACアドレスが付与されている。

【0032】

無線通信エリアAR1内に入ったコンピュータとしての端末50、60、70は、装着された無線LANアダプタ52、62、72とアクセスポイント20との間で電波が送受信されることにより、アクセスポイント20との通信を無線で行なう。アクセスポイント20および無線LANアダプタ52、62、72は、やり取りするデータを通信に適した形式、いわゆるパケットに変換することが可能であり、これにより、端末50、60、70とアクセスポイント20との間において、オフライン（インターネットに接続されていない状態）でデータのやり取りをすることが理論上可能となる。

【0033】

次に、アクセスポイント20をインターネットINに接続するための構成について説明する。図1に示すように、アクセスポイント20のWANポート24には、モデムを内蔵したルータ28がケーブルを介して接続されている。ルータ28は、無線LANアダプタ52、62、72それぞれのMACアドレスに基づいて、無線LAN内の複数の各端末50、60、70を特定し、これらを区別することができる。

【0034】

ルータ28内のモデムは、CATV回線、xDSL回線等のブロードバンドな通信回線CL、プロバイダPVの専用回線を介してインターネットINに接続されている。即ち、ルータ28は、無線LANをインターネットINに接続するゲートウェイとして機能する。

【0035】

なお、本実施例では、無線通信エリアAR1内にいる者が所有する無線LANアダプタを備えた端末のうち、MACアドレスがアクセスポイント20に登録されている端末（以下、登録端末という）に、無線LANへの接続を許容する。登録端末の所有者は、自己の端末をアクセスポイント20を通じてインターネットINに接続し、インターネットIN上のサーバSVに格納されたウェブコンテンツ等の種々の情報を取得することができる。一方、MACアドレスがアクセスポイント20に登録されていない端末（非登録端末という）は、たとえ無線通信エリアAR1内にいても無線LANに接続することができない。即ち、無線通信エリアAR1は、登録端末の所有者のみにインターネットINへの接続サービスを提供するフリースポットとされている。なお、図1では、端末50、60が登録端末に該当し、端末70が非登録端末に該当するものとする。

【0036】

こうした登録端末とアクセスポイント20との間では、契約やサービス等の種々の内容を有するデータ（以下、内容付きデータという）が電波に乗せて送受信される。本実施例では、内容付きデータを送信する側の装置（登録端末、アクセスポイント20）が、送信に先立って、既述したWEPキーという暗号鍵を用いて内容付きデータを暗号化し、暗号化後の内容付きデータ（以下、暗号化データという）を受信側の装置（アクセスポイント20、登録端末）に送信することとしている。受信側の装置は、受信した暗号化データをWEPキーを用いて復号化し、内容付きデータを得るのである。

【0037】

WEPは、IEEE802.11で使用される、秘密鍵暗号方式（データの暗号化と暗号化されたデータの復号化の双方で同じ暗号鍵を使用する方式）の暗号

化技術であり、暗号鍵として64ビットまたは128ビットのWEPキーが用いられる。

【0038】

こうしたWEPキーを用いた暗号化により、無線通信エリアAR1内において内容付きデータを乗せた電波が傍受された場合に、内容付きデータの解析がしにくくなり、通信内容の第三者への漏洩が防止される。例えば、登録端末からアクセスポイント20にクレジットカードの番号を含む契約文書が送信された場合には、送信電波の傍受によりクレジットカードの番号が第三者に知られてしまうことを防止することができる。

【0039】

A-2. WEPキーの設定に関する処理の内容：

続いて、上記のWEPキーを端末50、60に設定する手法について説明する。

【0040】

アクセスポイント20のROM12には、端末50、60との通信に関するプログラムとして、無線LANアダプタ52、62のMACアドレスの登録に関するプログラム（MAC登録プログラム）が予め格納されている。一方、無線LANの使用に際して端末50、60にインストールされたユーティリティプログラムには、WEPキーの設定に関するプログラム（WEPキー設定プログラム）が含まれている。

【0041】

上記のWEPキー設定プログラムの内容を端末50、60のCPUが実行し、このWEPキー設定プログラムの実行に伴って上記のMAC登録プログラムおよび出力値変更プログラムの内容をアクセスポイント20のCPU11が実行することにより、図3に示すセキュリティデータ設定処理が行なわれる。このセキュリティデータ設定処理が行なわれることにより、アクセスポイント20に無線LANアダプタ52、62のMACアドレスが登録され、アクセスポイント20および端末50、60に共通のWEPキーが設定される。

【0042】

セキュリティデータ設定処理の内容について図3ないし図4を説明する。図3はセキュリティデータ設定処理ルーチンを示すフローチャートである。図4は、出力値が変更された後の送信機25における電波の送信可能範囲を、セキュリティ通信エリアMR1として示す説明図である。この図3ないし図4に関する以下の説明では、MACアドレスの登録対象ないしWEPキーの設定対象となる端末が端末50であると仮定して説明する。

【0043】

セキュリティデータ設定処理ルーチンは、端末50側のCPUで実行されるルーチンAとアクセスポイント20側のCPU11で実行されるルーチンBとからなる。本ルーチンによる登録に先立ち、アクセスポイント20の管理者は、端末50がセキュリティ通信エリアMR1内にあることを確認して登録ボタン127を作動させる（ステップS200、S210）。セキュリティ通信エリアMR1は、既述した出力値変更プログラムの実行によって標準設定値が一時的に低減された場合に、送信機25による電波の送信が可能となる範囲である（図4を参照）。上記の登録ボタン127の作動により、アクセスポイント20は、既述した出力値変更プログラムを実行して、送信機25の出力値を標準設定値の $1/n$ に低減する処理を行なう（ステップS220）。これにより、送信機25が電波を送信できる範囲は、図4に示すセキュリティ通信エリアMR1内となり、無線通信エリアAR1よりも狭くなる。従って、無線通信エリアAR1内に入っている登録端末であっても、セキュリティ通信エリアMR1内に入っていない場合には、アクセスポイント20にアクセスすることができなくなる。

【0044】

次に、端末50は、無線LANアダプタ52のMACアドレスを特定し、無線LANに加入する旨の指示（以下、加入指示という）を表わすデータにMACアドレスをヘッダ情報として付加したパケットを、アクセスポイント20に送信する処理を行なう（ステップS100）。

【0045】

続いて、受信したパケットのヘッダ情報からMACアドレスを読み取り、読み取ったMACアドレスをRAM13のバッファ領域に一時的に記憶する処理を行

なう（ステップS230）。

【0046】

続いて、使用するWEPキーを表わすデータ（以下、WEPキーデータという）を端末50に送信する処理を行ない（ステップS250）、WEPキーデータが端末50に配信されたか否かを判断する処理を行なう（ステップS255）。この配信されたか否かの判断は、既述した無線LANアダプタ52のデータリターン機能を利用することにより実現することができる。WEPキーデータが端末50に配信されていないと判断した場合には、RAM13に記憶されていたMACアドレスを消去し（ステップS260）、本ルーチンを終了する。

【0047】

一方、WEPキーデータが端末50に配信されたと判断した場合には、既述した出力値変更プログラムを実行して、送信機25の出力値を標準設定値に戻す処理を行なう（ステップS270）。これにより、送信機25が電波を送信できる範囲が、通常の範囲（無線通信エリアAR1）となり、登録端末は、無線通信エリアAR1内に入っていれば、アクセスポイント20にアクセスすることができる。

【0048】

続いて、端末50のMACアドレスを、記憶装置14の管理領域に登録する処理を行なう（ステップS280）。これにより、アクセスポイント20側での端末50に関するMACアドレスの登録が完了する。

【0049】

一方、ステップS250の処理によってWEPキーデータを受信した端末50は、WEPキーをアクセスポイント20のIPアドレスと関連付けて自動的に設定する処理を行ない（ステップS110）、本ルーチンを終了する。これにより、端末50側でのアクセスポイント20に関するWEPキーの設定が完了する。以降、端末50とアクセスポイント20との間では、設定されたWEPキーを用いて内容付きデータを暗号化した暗号化データが送受信される。

【0050】

A-3. 作用効果：

以上説明した第1実施例の暗号鍵設定システムLH1では、上記のセキュリティデータ設定処理を実行することにより、端末50にWEPキーを自動的に設定する。このような「WEPキーの無線通信による自動設定」がなされることで、無線LANを利用する端末50の新規追加を簡便に実現することが可能となり、加入し易い無線LANを提供することができる。例えば、WEPキーの設定に際し、端末50の所有者やアクセスポイント20の管理者は、端末50とアクセスポイント20とをケーブル等で接続する必要がなく、また、WEPキーの作成や設定を手作業で行なう必要もない。特に、上記の暗号鍵設定システムLH1をフリースポットに備えられた無線LANに採用すれば、なお好適である。フリースポットの無線LANは、これを利用しようとする多数の人が次々と新規に加入するものであり、各人の設定に伴って必要な作業を大きく軽減することができるからである。

【0051】

更に、アクセスポイント20は、WEPキーのデータを電波に乗せて端末50に送信する際に、アクセスポイント20から送信される電波が届く範囲を、通常範囲である無線通信エリアAR1から、より狭い範囲であるセキュリティ通信エリアMR1に変更する。このため、WEPキーデータに乗せた電波が傍受される可能性が低くなる。例えば、図4において、アクセスポイント20から端末50にWEPキーデータが送信された場合に、WEPキーデータに乗せた電波は、狭い範囲であるセキュリティ通信エリアMR1内にしか届かず（矢印Q1を参照）、セキュリティ通信エリアMR1外にいる登録端末60や非登録端末70に受信されてしまうことがない。従って、上記のようにWEPキーデータが無線で送信される場合であっても、WEPキーの漏洩を防止することが可能となり、セキュリティレベルの高い無線LANを実現することができる。特に、このようなアクセスポイント20をフリースポットに設置した場合には、フリースポットを利用しようとする多数の者の端末について、WEPキーの設定時にWEPキーが第三者に漏洩してしまうことが確実に防止される。従って、多数の各利用者の通信の秘密を十全に確保することができる。

【0052】

また、第1実施例の暗号鍵設定システムLH1では、アクセスポイント20は、端末50からの加入指示を表わすデータの受信に伴って一時的に通信範囲を狭めてWEPキーを作成し、作成したWEPキーの端末50への送信後に通信範囲を元に戻している。従って、端末50の所有者は、アクセスポイント20に触れることなくWEPキーの設定を行なうことが可能となり、簡便かつ衛生的である。

【0053】

第1実施例の暗号鍵設定システムLH1では、アクセスポイント20が、WEPキーの設定に併せて端末50側のMACアドレスを登録し、登録端末50、60についてのみ無線LANへの接続を許容する。これにより、非登録端末70による無線LANへの接続を簡便な手法で防止することができる。また、非登録端末70がLAN上の登録端末50、60やアクセスポイント20に侵入してWEPキーのデータ等の各種のデータを取得することを未然に防止することができる。

【0054】

上記第1実施例において、通信範囲を狭める期間としては、(a)登録ボタン127が押されている間、(b)登録ボタン127を押してからMACアドレスおよびWEPキーが登録されるまでの間、(c)登録ボタン127を押してからもう一度押すまでの間等が考えられる。また、通信範囲を狭めるトリガーとして、前記登録ボタン127によらずに、アクセスポイント20が端末50から加入指示を表わすデータを受信したときとしてもよい。この場合は、該端末50がセキュリティ通信エリアMR1内にあることを、通信の応答時間で判別することも可能である。

【0055】

B. 第2実施例（暗号鍵設定システムLH2）：

次に、第2実施例について説明する。第1実施例では、WEPキーのデータが乗った電波が傍受されることを、WEPキーの設定の際に通信範囲を一時的に狭めるというソフト的な手法で防止した。これに対し、第2実施例の暗号鍵設定システムLH2では、WEPキーのデータが乗った電波が傍受されることを、「ア

クセスポイント 2 0 および端末 5 0 を覆うシールド箱 9 5」というハード的な手法で実現する。

【 0 0 5 6 】

図 6 は本発明の第 2 実施例である暗号鍵設定システム L H 2 を実現する装置構成を示す説明図である。アクセスポイント 2 0 および端末 5 0, 6 0, 7 0 は、第 1 実施例とほぼ同様の構成を備え、このアクセスポイント 2 0 によって第 1 実施例と同様の無線通信エリア A R 1 が形成されている。図 6 に示すように、アクセスポイント 2 0 および端末 5 0 は、敷板 9 6 の上に配置されている。この敷板 9 6 には、アクセスポイント 2 0, 端末 5 0 を包摂可能な中空部を有するシールド箱 9 5 が覆い被せられている。シールド箱 9 5 および敷板 9 6 は鉄等の金属で形成されている。

【 0 0 5 7 】

第 2 実施例では、W E P キーの設定を以下の手順で行なう。まず、無線 L A N への加入を希望する者は、アクセスポイント 2 0 の設置場所に行き、自己の所有する端末 5 0 とアクセスポイント 2 0 を敷板 9 6 の上に配置する。このとき、敷板 9 6 の上には予めアクセスポイント 2 0 が配置されていることとしても差し支えない。次に、無線 L A N への加入を希望する者は、端末 5 0 を操作して無線 L A N に加入する旨の指示を行なった後、敷板 9 6 にシールド箱 9 5 を被せる。アクセスポイント 2 0 は、端末 5 0 から加入指示を表わすデータを受信し、該受信から所定時間（例えば、シールド箱 9 5 を被せるのに要する時間）の経過後に、第 1 実施例と同様の M A C アドレスの登録処理や W E P キーの設定処理（ステップ S 1 0 0, ステップ S 2 3 0, ～ステップ S 2 6 0, ステップ S 2 8 0, ステップ S 1 1 0 の各処理）を行なう。これにより、アクセスポイント 2 0 側での端末 5 0 に関する M A C アドレスの登録が完了し、アクセスポイント 2 0 で作成された W E P キーのデータが端末 5 0 に送信されて端末 5 0 への W E P キーの設定が完了する。

【 0 0 5 8 】

以上説明した第 2 実施例の暗号鍵設定システム L H 2 では、W E P キーの設定の際、W E P キーのデータをやり取りする端末 5 0 およびアクセスポイント 2 0

がシールド箱 9 5 によって遮蔽される。このため、W E P キーデータを乗せた電波が傍受されることを確実に防止することができる。例えば、図 6 において、アクセスポイント 2 0 から端末 5 0 に W E P キーデータが送信された場合に、W E P キーデータを乗せた電波は、シールド箱 9 5 を通り抜けることができないので（矢印 Q 2 を参照）、無線通信エリア A R 1 内の登録端末 6 0 や非登録端末 7 0 に受信されてしまうことがない。また、無線通信エリア A R 1 内の登録端末 6 0 や非登録端末 7 0 が、W E P キーデータが乗った電波を傍受しようとした場合であっても、電波はシールド箱 9 5 を通り抜けることができないので（矢印 Q 3 を参照）、W E P キーデータが乗った電波をキャッチすることができない。従って、W E P キーデータが無線で送信される場合であっても、W E P キーデータの漏洩を防止することが可能となり、セキュリティレベルの高い無線 L A N を実現することができる。

【 0 0 5 9 】

C. 変形例：

以上本発明の実施の形態を実施例に基づいて説明したが、本発明はこうした実施例に何等限定されるものではなく、本発明の要旨を逸脱しない範囲内において種々なる様態で実施し得ることは勿論である。

【 0 0 6 0 】

例えば、上記実施例では、アクセスポイント 2 0 に外部アンテナを有線で接続し、外部アンテナと端末 5 0 との無線での通信によって M A C アドレスの登録や W E P キーの設定を行なう構成としても差し支えない。こうすれば、アクセスポイント 2 0 の設置場所の自由度を高めることができる。例えば、店内の隅に外部アンテナを設置して外部アンテナの近辺を W E P キーの設定場所としつつ、店内の中央にアクセスポイント 2 0 を設置して無線通信エリアを店内の全体に広く確保することができる。

【 0 0 6 1 】

上記実施例では、端末とアクセスポイントとの間でやりとりされるデータの内容を暗号化する技術として W E P を用いたが、W E P 以外の他の暗号化技術を用いても差し支えない。例えば、公開鍵暗号方式（データの暗号化と暗号化された

データの復号化とで異なる暗号鍵を使用する方式)の暗号化技術を用いてもよい。また、WEPよりも強度の高い暗号化技術であるWPA(Wi-Fi Protected Access)を用いることも考えることができる。

【0062】

また、上記実施例では、WEPキーの設定中における無線通信範囲を限定したが、このような無線通信範囲の限定は、WEPキーのみならず、アクセスポイント20と端末50との間のやり取りによって設定される他の情報にも適用することができる。例えば、特定の人に対してのみ有料コンテンツを送信するフリースポットでは、アクセスした端末の所有者が特定の人であることを認証するための情報(例えば、端末所有者の氏名、IDやパスワード等)をアクセスポイント20や端末50に予め登録する場合がある。こうした個人を認証する情報の登録を、アクセスポイント20と端末50との間の無線通信範囲を限定しつつ、無線通信によって行なう構成としてもよい。こうすれば、IDやパスワード等の個人を認証する情報をマニュアルで設定する必要がない。

【図面の簡単な説明】

【図1】 本発明の第1実施例である暗号鍵設定システムLH1を実現するハードウェアの構成を示す説明図である。

【図2】 アクセスポイント20の構成を示す説明図である。

【図3】 セキュリティデータ設定処理ルーチンを示すフローチャートである。

【図4】 出力値が変更された後の送信機25における電波の送信可能範囲を、セキュリティ通信エリアMR1として示す説明図である。

【図5】 本発明の第2実施例である暗号鍵設定システムLH2を実現する装置構成を示す説明図である。

【符号の説明】

11…CPU

12…ROM

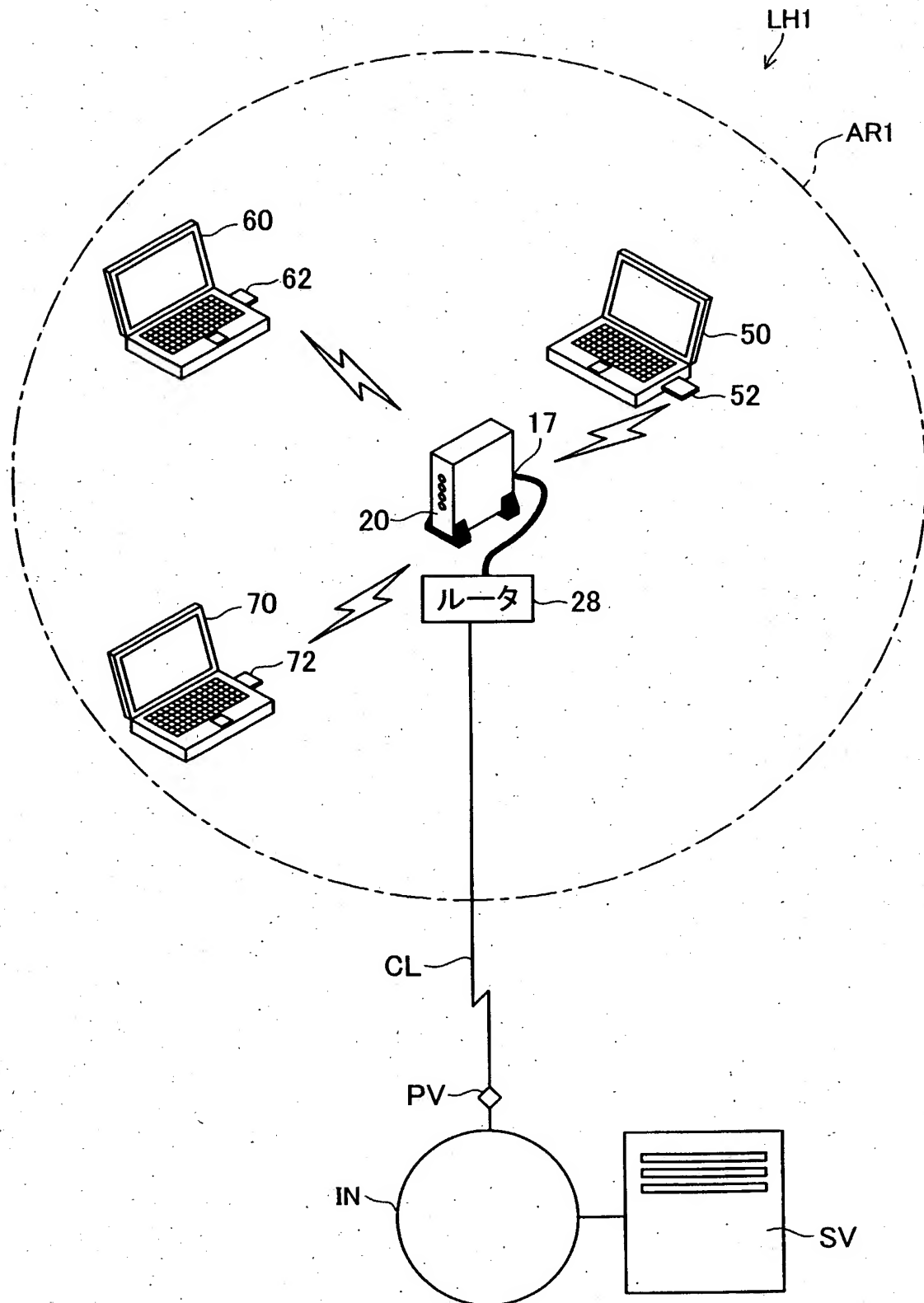
13…RAM

14…記憶装置

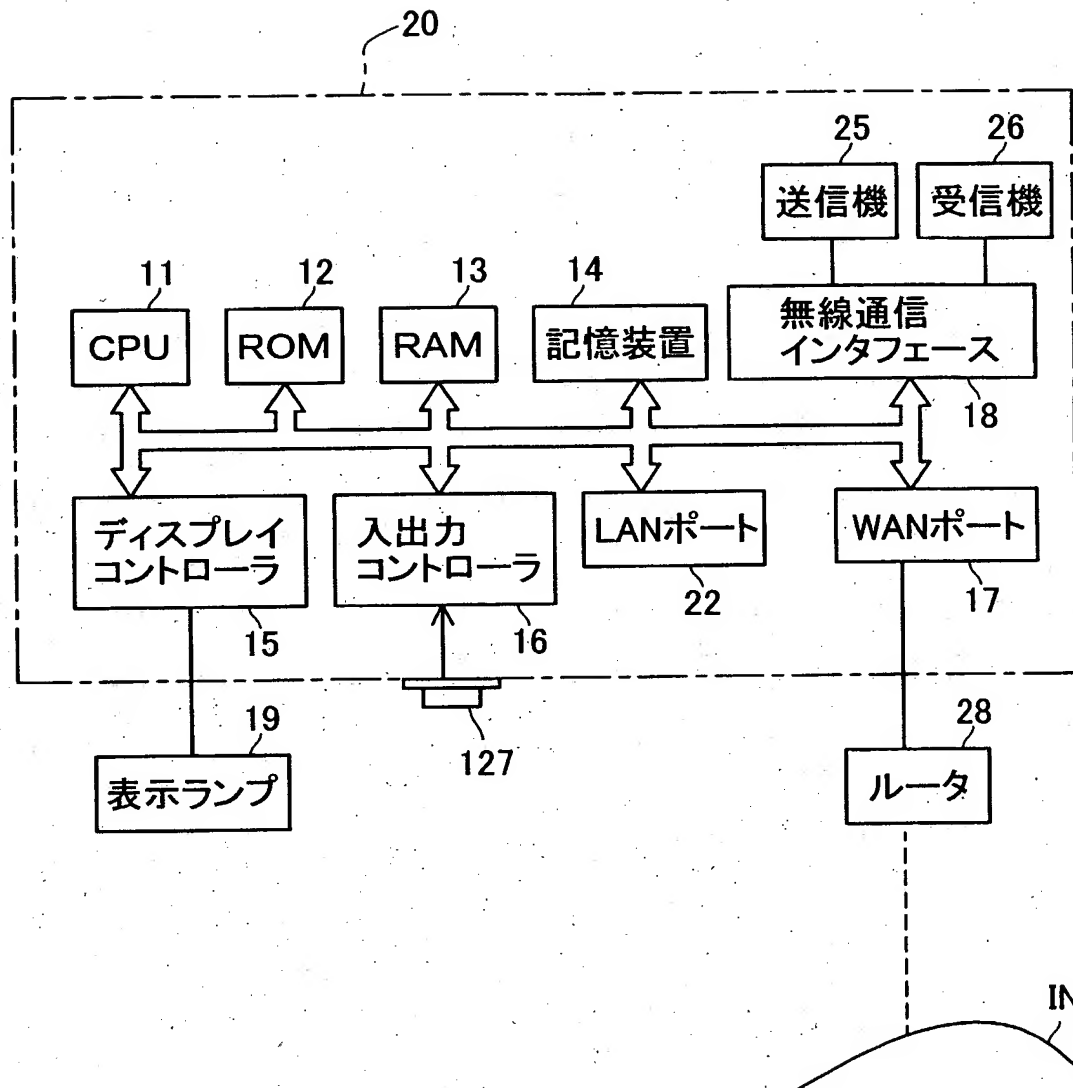
- 1 5 …ディスプレイコントローラ
- 1 6 …入出力コントローラ
- 1 7 …WANポート
- 1 8 …無線通信インタフェース
- 1 9 …表示ランプ
- 2 0 …アクセスポイント
- 2 2 …LANポート
- 2 5 …送信機
- 2 6 …受信機
- 2 8 …ルータ
- 5 0, 6 0, 7 0 …端末
- 5 2, 6 2, 7 2 …無線LANアダプタ
- 9 5 …シールド箱
- 9 6 …敷板
- 1 2 7 …登録ボタン
- AR 1 …無線通信エリア
- CL …通信回線
- IN …インターネット
- LH 1, LH 2 …暗号鍵設定システム
- MR-1 …セキュリティ通信エリア
- PV …プロバイダ
- SV …サーバ

【書類名】 図面

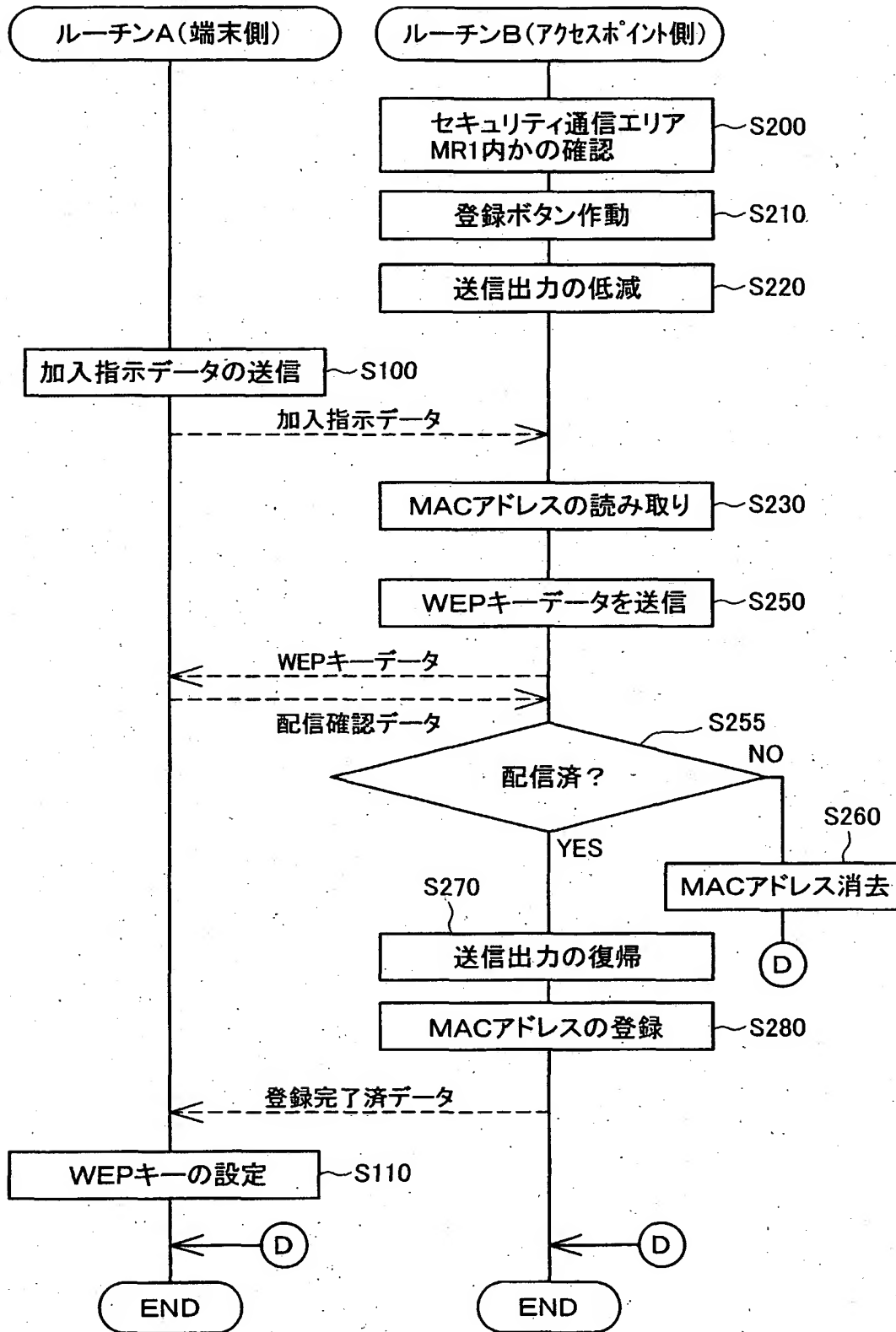
【図1】



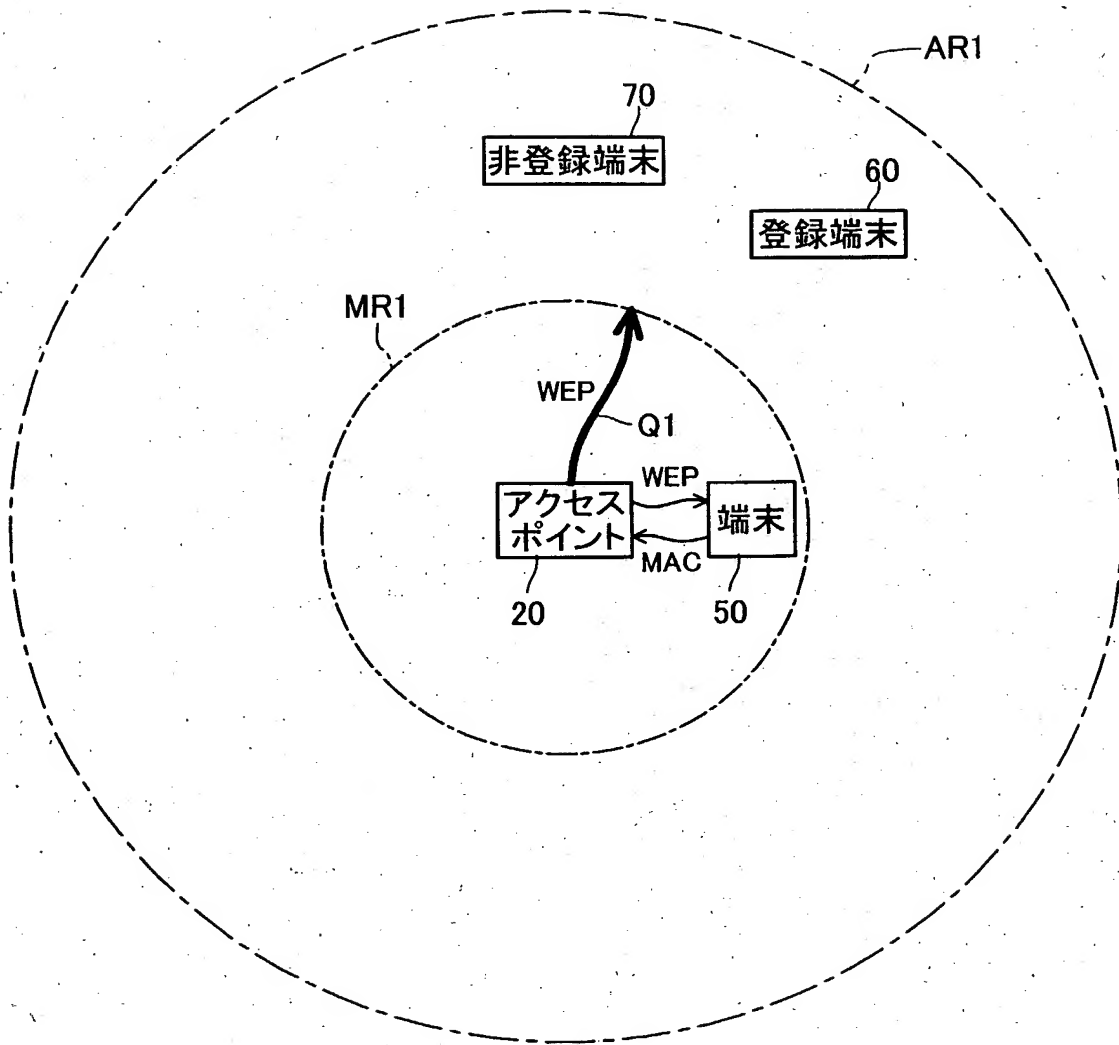
【図2】



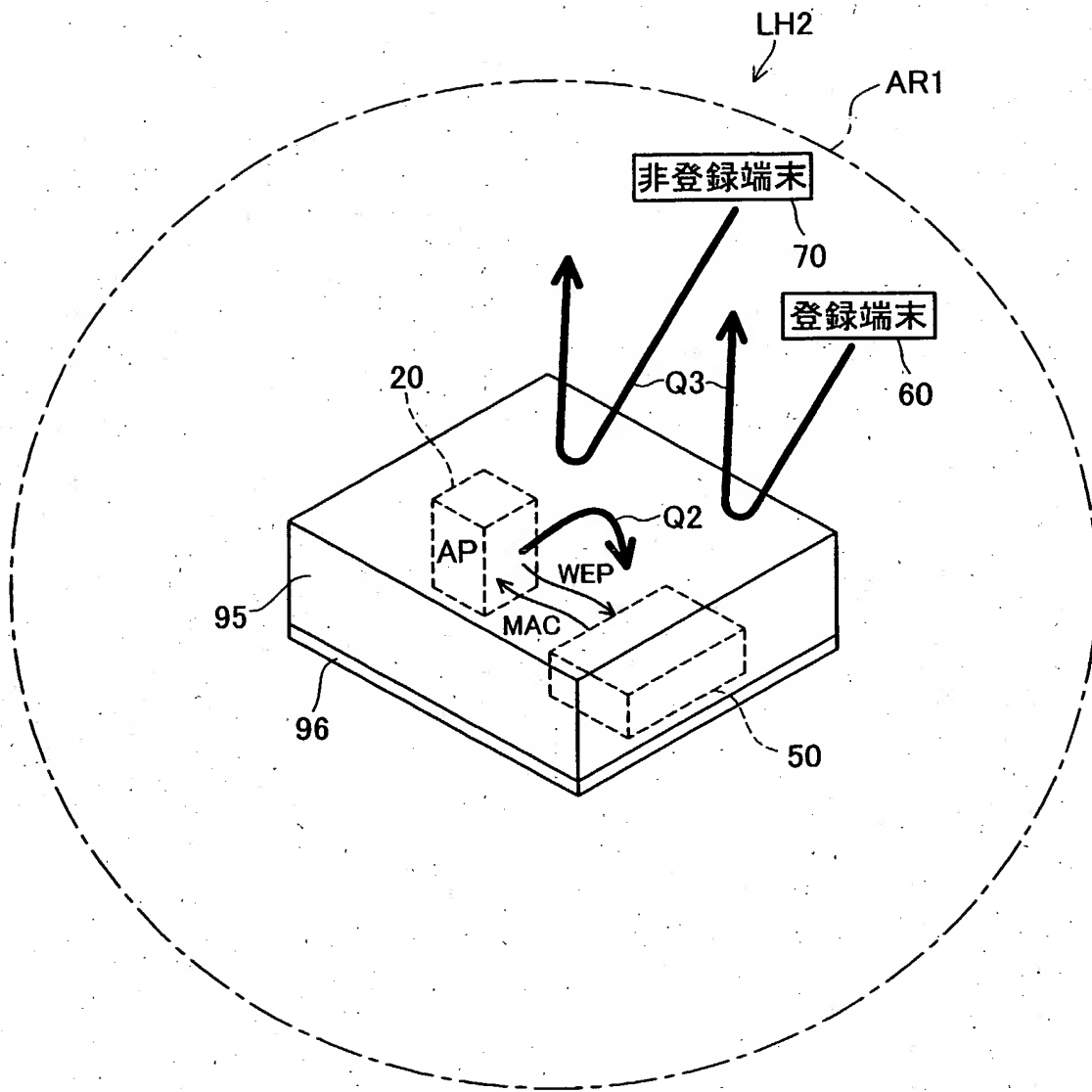
【図 3】



【図4】



【図5】



【書類名】 要約書

【要約】

【課題】 無線LANを利用する端末の新規追加を、暗号鍵を表わすデータの漏洩を防止しつつ、簡便な手法で実現することを目的とする。

【解決手段】 アクセスポイント20は、登録ボタン127の作動により、アクセスポイント20から送信される電波が届く範囲を、通常範囲である無線通信エリアAR1から、より狭い範囲であるセキュリティ通信エリアMR1に変更する。この後、アクセスポイント20は、使用されるWEPキーを端末50に配信し、配信確認の後、端末50のMACアドレスを登録する。端末50は配信されたWEPキーを自己に設定する。

【選択図】 図3

出 願 人 履 歴 情 報

識別番号 [390040187]

1. 変更年月日 1990年12月10日

[変更理由] 新規登録

住 所 愛知県名古屋市中区大須4丁目11番50号

氏 名 株式会社メルコ